REMARKS/ARGUMENTS

The Examiner rejected claims 1-4, 7-30, and 33-40 as anticipated (35 U.S.C. §102) by Ananda (U.S. Patent No. 5,495,411). Applicants traverse for the following reasons.

Independent claims 1, 16, and 27 concern distributing computer software from a first computer system, and require: receiving a request for software from a second computer system; generating a message; encrypting the generated message; transmitting the encrypted message to the second computer system; receiving an encrypted response from the second computer system; determining whether there is a code made available by the second computer system capable of decrypting the received encrypted response; decrypting the encrypted response with the determined code if there is one determined code; processing the decrypted response to determine whether the second computer system is authorized to access the software; and permitting the second computer system access to the software after determining that the second computer system is authorized to access the software.

Applicants amended independent claims 1 and 16 to clarify that the first computer system performs the claimed operations, which requirement is already found in claim 27.

The Examiner cited col. 11, lines 45-60 and col. 12, lines 14-53 as disclosing the requirements of these claims. (Office Action, pgs. 2-3) Applicants traverse.

According to Ananda, when the user initiates execution of the application 310, the rental security manager 321 in the user computer is activated to initiate the authorization verification process by obtaining a current time from the user computer 102, which is the local processor clock time. (Ananda, col. 10, lines 43-55) The user computer 150 includes header software 320 coupled to the application, which is used to prevent unauthorized use. The header software 320 in the user computer has a rental security manager 321 that determines whether the user may continue to access the software. (Ananda, col. 9, lines 56 to col. 10, line 15).

In response to receiving an authorization verification message f, the multiuser controller 222 of the central facility 180 decrypts the message from the user rental security manager 321 to obtain the user processor clock time and software ID, and determine the time difference between the transfer time and the user processor clock time. (Ananda, col. 10, lines 63 to col. 11, line 7) Both the central facility controller 22 and user rental security manager 321 use the same

password generation module algorithm to generate a password based on the time difference and the user ID. (Col. 11, lines 9-30)

The rental security manager 321 in the user computer generates an authorization verification password based on the user processor clock time, the user ID password and the application ID that is encrypted and sent to the multiuser controller at the central facility 180. (Col. 11, lines 45-60) The multiuser controller 22 decrypts the message, and computes the time difference between the user processor clock time and the transfer time stored, and then uses the algorithm to generate the password, or pseudo random number parameter. The multiuser controller 22 encrypts this message and sends to the user rental security manager 321, which then decrypts this message, and then uses a password validation module to determine whether the correct verification password was sent by the multiuser controller 222. (Ananda, col. 12, lines 15-50)

Applicants submit that the cited Ananda does not disclose many claim requirements of claims 1, 16, and 27 for the following reasons.

Nowhere does the cited Ananda anywhere disclose a method, system or program for distributing computer software from a first computer system to a second computer system as claimed in the preamble. Instead, Ananda concerns a technique to allow a user to run already installed software. According to Ananda, "[w]hen the user initiates execution of the application software 310, the execution command initiates the application software 310 which in turn initiates the processing of the header software 320. This activates the rental security manger 321 to initiate the process of authorization verification." (Ananda, col. 10, lines 43-50) Thus, the cited Ananda concerns enabling access to already installed software not distributing computer software from a first to second computer systems as claimed.

Nowhere does the cited Ananda disclose that the first computer system, which controls access to the software, process the decrypted response to determine whether the second computer system is authorized to access the software. The section of Ananda, col. 12, lines 36-46, that the Examiner cited for this claim requirement (Office Action, pg. 2) mentions that the user computer rental security manager 321 receives the encrypted message, decrypts it, and then compares the decrypted message against stored information to determine whether the received decrypted message authorizes the application to continue executing. (Ananda, col. 12, lines 36-54) The

cited Ananda has the user computer system, which the Examiner likens to the second computer system that accesses the software, determine whether the message provides access. This is different from and does not disclose the claim requirement that the first computer system performs the operations to determine whether the second computer system may access the software when processing the decrypted response. Instead, the cited Ananda has the user computer system, likened to the second computer system, decrypt the response to determine whether the application may continue running.

Moreover, nowhere does the above cited Ananda disclose the requirement of determining whether there is a code made available by the second computer system capable of decrypting the received encrypted response and decrypting the encrypted response with the determined code if there is one determined code, and that the decrypted response is processed to determine whether the second computer system is authorized to access the software. Instead, the cited cols. 11 and 12 of Ananda mention that the user and central facility sides encrypt and decrypt messages sent back and forth using an encryption decryption method (DEM) algorithm. (Ananda, col. 10, lines 55-60; Col. 11, lin 19-22; col. 12, lines 18-21; 40-43). Nowhere does the cited Ananda anywhere disclose the requirement that to perform the decryption of a message used to grant access to software, the first computer system, which the Examiner likens to the central facility, determines whether there is a code made available by the second computer system (likened to the user computer) that the first computer system (e.g., central facility) uses to decrypt the received encrypted response.

Accordingly, claims 1, 16, and 27 are patentable over the cited art because the cited art does not disclose all the requirements of these claims.

Claims 2-4, 8-11, 17-19, 21-24, 28-30, and 34-40 are patentable over the cited art because they depend, directly or indirectly, from one of claims 1, 16, and 27. Moreover, certain of these claims provide additional grounds of patentability over the cited art for the reasons discussed below.

Claims 3, 18, and 29 depend from claims 1, 16, and 27 and further require transmitting the software to the second computer system after permitting access. The Examiner cited col. 12, lines 47-53 of Ananda as disclosing the requirement of these claims. (Office Action, pg. 3) Applicants traverse.

The cited col. 12 mentions that if the authorization is verified, the application software can continue executing. Nowhere does this cited Ananda anwhere disclsoe that the first computer system transmit the software to the second computer system as claimed. Instead, the cited Ananda mentions how verification permits the software to run, and does not mention transmitting the software to the second computer system when access is verified.

Accordingly, amended claims 3, 18, and 29 provide additional grounds of patentability over the cited art.

Amended claims 4, 19, and 30 depend from claims 1, 16, and 27, respectively, and further require that generating the message further comprises generating a random component to include within the message, and that determining whether the second computer system is authorized to access the software further comprises determining whether the decrypted response includes the generated message transmitted to the second computer system, wherein the second computer system is authorized to access the software if the decrypted response includes the generated message.

Nowhere does the cited Ananda anywhere disclose that the first computer system determines whether the second computer system is authorized to access the software by determining whether the decrypted response includes a generated message the first computer system sent to the second computer system.

Instead, with the cited Ananda, the multiuser controller 222, likened to the first computer system, receives an encrypted message from the user rental security manager 321, likened to the second computer system, having the processor clock time, user ID, and identification number. (Col. 11, line 60 to col. 12, line 14) The multiuser controller 222 then uses the information from the user computer rental service manager 321 to generate a message having a pseudo random number, which is sent to the rental service manager 321 on the user computer to verify whether the software may continue executing. (Ananda, col. 12, lines 14-54)

The above cited Ananda does not have the first computer system sending a generated to the second computer system, where the second computer system encrypts the generated message from the first computer system and sends the encrypted generated message back to the first computer system to determine whether access is permitted. Instead, the above discussed Ananda has the multiuser controller 222, which is likened to the first computer system, send the random

number to the user computer, likened to the second computer system, where the second computer system, not the first as claimed, determines whether access is permitted. Thus, Ananda has the user computer attempting to gain access determine whether the random component permits access. This is the opposite of the claims which has the system controlling access, the first computer system that is separate from the second computer system requesting access, receive a random message from the user computer seeking access, i.e., the second computer system and then determining whether access is permitted. In other words, the claims require the system managing access receive a random component it previously sent to the user system seeking access to determine whether access is allowed. The cited Ananda, on the other hand, has the system controlling access send a random component to the user system seeking access so the user system can determine whether access is permitted.

Accordingly, amended claims 4, 19, and 30 provide additional grounds of patentability over the cited art.

Claims 7, 20, and 33 depend from claims 1, 16, and 27 and further require the software comprises a computer program and automatically causing the installation of the computer software on the second computer system when the computer software is transmitted to the second computer system.

The cited col. 12, lines 47-53 of Ananda (Office Action, pg. 3) mentions that the software is allowed to continue executing if the password is verified. Nowhere does the cited Ananda anywhere disclose the claim requirement of automatically causing the installation of the computer software on the second computer system when the computer software is transmitted to the second computer system when the password is verified..

Accordingly, amended claims 7, 20, and 33 provide additional grounds of patentability over the cited art.

Claims 8, 21, and 34 depend from claims 1, 16, and 27, respectively, and further require that processing the encrypted response further comprises determining whether a message included in the encrypted response matches the generated message, wherein the second computer is authorized to access the software if the message included in the encrypted response matches the generated message.

The cited Ananda does not disclose that the first computer system determines whether the message in the encrypted response from the second computer system matches the generated message the first computer system initially sent to the second computer system. Instead, the cited Ananda has the user computer system compare stored information with a message from the central facility, likened to the first computer system, to determine whether access is permitted. Nowhere does the cited Ananda anywhere disclose that the central facility, likened to the first computer system, compare a message in an encrypted response from the user computer, likened to the second computer system, to determine whether it matches the generated message the central facility (first computer system) previously sent to the user computer (second computer system). Thus, the cited operations of Ananda are different from the claimed operations.

Accordingly, claims 8, 21, and 34 provide additional grounds of patentability over the cited art.

Claims 9, 11, 14, 22, 24, 26, 35, and 37 depend from base claims 1, 16, and 27, and additionally require that the message transmitted to the second computer system is encrypted with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system and that the encrypted response from the second computer system is encrypted with the second computer system's private key, wherein the first computer system has a public key of the second computer system for decrypting the encrypted response.

These claims also included the added requirement in the amendment that the code made available by the second computer system that is capable of decrypting the received encrypted response comprises the public key associated with the second computer system.

The Examiner cited the above discussed Ananda as disclosing the additional requirements of these claims. (Office Action, pgs. 2-3.). For the reasons discussed above, the cited Ananda nowhere discloses the claim requirement of determining whether there is a code made available by the second computer system capable of decrypting the received encrypted response, nor do these cited sections disclose that the code made available by the second computer system that is capable of decrypting the received encrypted response comprises a public key associated with the second computer system as claimed.

The Examiner further mentioned the user processor clock included in a message from the user computer rental security manager 321 to the central facility. (Office Action, pg. 3) Nowhere does this cited user processor clock, which is provided to use to generate the password, anywhere disclose that the second computer system provide a code capable of decrypting messages from the second computer system. Instead, the user clock is used to independently generate the pseudo random number used for verification, not decrypt messages as claimed.

Accordingly, amended claims 9, 11, 14, 22, 24, 26, 35, and 37 provide additional grounds of patentability over the cited art.

Independent claims 12 and 25 concern accessing computer software from a first computer system with a second computer system and require that the second computer system perform: providing a code to the first computer system capable of decrypting an encrypted response from the from the second computer system; transmitting a request for the software to the first computer system; receiving an encrypted message from the first computer system; processing the encrypted message to generate a response message; encrypting the response message, wherein the encrypted response message is capable of being decrypted by the provided code at the first computer system; transmitting the encrypted response message to the first computer system; and receiving access to the requested software in response to the encrypted response message.

Applicants amended claims 12 and 25 to clarify the operations are performed by the second computer system attempting to access the software.

The Examiner cited the same sections of Ananda against claims 12 and 25 that were cited against independent claims 1, 16, and 27. Applicants submit that claims 12 and 25 further distinguish over the cited Ananda because they require providing a code to the first computer system capable of decrypting an encrypted response from the second computer system that includes a message from the first computer system, and encrypting the response message, wherein the encrypted response message is capable of being decrypted by the provided code at the first computer system.

For the reasons discussed above with respect to claims 1, 16, and 27, the cited Ananda does not disclose the claim requirements of providing a code to the first computer system capable of decrypting a received encrypted response from the second computer system that includes a message the first computer system sent to the second computer system in an encrypted message

to access the requested software that the second computer system, in turn, returns in the encrypted response to the first computer system to access the requested software.

Accordingly, claims 12 and 25 are patentable over the cited Ananda because Ananda does not disclose the claim requirements.

Claims 13-15 and 26 are patentable over the cited art because they depend from claims 12 and 25, respectively, which are patentable over the cited art for the reasons discussed above.

Claims 38-40 are patentable over the cited art because they depend, directly or indirectly, from claim 26, which is patentable over the cited art for the reasons discussed above.

The Examiner rejected claims 5, 6, 31, and 32 as obvious (33 U.S.C. 103) over Ananda in view of Komura (U.S. Patent No. 5,994,307). Applicants traverse this rejection on the grounds that these claims depend from claims 1, 16, and 27, which are patentable over the cited art for the reasons discussed above. Moreover, these claims provide additional grounds of patentability over the cited art for the reasons discussed below.

First off, claims 5, 6, 31, and 32 are patentable over the cited art because they depend from claims 1, 16, and 27, which are patentable over the cited art for the reasons discussed above. Further, these claims provide additional grounds of distinction over the cited art for the following reasons.

Claims 5 and 31 depend from claims 1 and 27, respectively, and further require that the random component is comprised of a time stamp. The Examiner cited Komura as teaching the time stamp claim requirement. (Office Action, pg. 4) Applicants traverse.

Although the cited Komura does discuss a timestamp and Ananda mentions that a clock time is used to calculate a pseudo number password, nowhere does the cited Ananda or Komura, alone or in combination, anywhere teach or suggest that a message generated and encrypted and sent to a second computer system, which is then included in an encrypted response by the second computer system to the first computer system, comprises a timestamp.

Accordingly, claims 5 and 31 provide additional grounds of patentability over the cited art.

Claims 6 and 32 depend from claims 5 and 31 and further require that the time stamp is inserted at an offset into the message. These claims are patentable over the cited combination because they depend from claims 5 and 31, which are patentable over the cited art for the reasons

discussed above, and because they provide further requirements on the timestamp, which is not disclosed in the cited Ananda.

Conclusion

For all the above reasons, Applicant submits that the pending claims 1-40 are patentable over the art of record. Applicants have not added any claims. Nonetheless, should any additional fees be required, please charge Deposit Account No. 09-0466.

The attorney of record invites the Examiner to contact him at (310) 553-7977 if the Examiner believes such contact would advance the prosecution of the case.

Dated: June 7, 2004
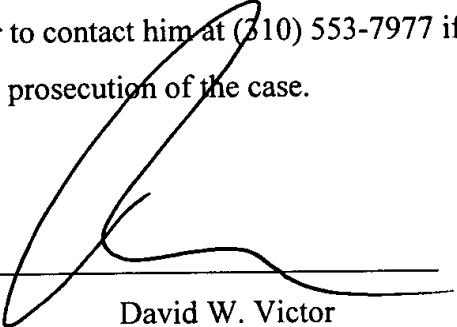
By: _____
David W. Victor
Registration No. 39,867

Please direct all correspondences to:

David Victor
Konrad Raynes Victor & Mann, LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, CA 90212
Tel: 310-553-7977
Fax: 310-556-7984